



IDENTITY THEFT

what you need to know



Step By Step: What To Do After a Security Breach

#1: Place a fraud alert on your credit reports.

It's **FREE**, stays in place for 90-days and requires potential creditors to take steps to verify that the applicant is in fact you.

You **only have to contact 1** of the 3 credit reporting agencies (CRA) to place the alert. Once you place the alert, you will receive notice that you can get 1 **FREE** copy of your credit report from **each** of the CRAs. It is a great idea to request all three reports and make sure that everything on them is accurate.

Equifax: 800-685-1111

TransUnion: 800-680-7289

Experian: 888-397-3742

#2: Consider placing a security freeze on your credit reports.

It's **FREE** and will prevent

potential creditors and other third parties from accessing your credit report for new products or services, unless you temporarily lift the freeze. **You must call each of the CRAs to do this.** It is **FREE** to place, thaw and lift the freeze for SC residents. Once you place the freeze, you will receive a personal identification number (PIN) you can use to thaw or lift the freeze. Make sure to keep it in a safe place. For more information on the freeze, including *how to place, thaw and lift one*, see page 3.

#3: Monitor your financial and personal statements closely.

Ensure that your bills and statements are arriving on time and are completely accurate. Remember, identity thieves can use your social

security number the same way you do. Including to receive:

- Government benefits
- Driver's License/ID
- Tax refund
- Medical benefits

So, monitor medical and benefits statements and always be on alert for any suspicious or unexpected letters or phone calls!

#4: Interested in a monitoring service?

Think you might need some help keeping track of everything? Monitoring services typically offer to do what you can freely do yourself (*see steps 1-3 above*). Just remember to research the company to ensure they are (1) TRUSTWORTHY, RELIABLE and LEGIT and (2) their services fit your needs.

WHAT'S INSIDE:

Learn What
Tools are at
YOUR Disposal

page 2

How to Place,
Thaw & Lift a
Security Freeze

page 3

Are YOU a
Victim of
Identity Theft?

page 5

Fraud Alerts, Freezes and Credit Report Monitoring, OH MY! So, What's the Difference?

Here is a more thorough rundown of the tools we covered on page 1.

FRAUD ALERT:

WHAT IS IT? Federal law gives consumers the right to place a fraud alert on credit reports for **FREE**. It alerts potential creditors pulling your report to take extra steps to verify your identity before issuing credit or services in your name.

HOW LONG WILL IT LAST? Lasting 90 days, the alert entitles you to another free credit report from each of the three credit reporting agencies. While an initial fraud alert can be renewed, if you have proof you are a victim of identity theft, you can place an extended fraud alert that lasts 7 years.

WHO DO I CONTACT? You only have to contact one of the credit reporting agencies and they'll notify the other two. Equifax (800-685-1111; press 2, then 1) or TransUnion (800-680-7289, press 1) or Experian (888-397-3742, press 2, 2, 1 then 2).

SECURITY FREEZE:

WHAT IS IT? When a freeze is in place, a business that receives an application for products or services cannot access your credit report without your permission. Utilities, credit cards and insurance all commonly require a credit check. A freeze doesn't affect your existing lines of credit and will need to be thawed if you decide to apply for new credit or services.

HOW LONG DOES IT LAST? The freeze lasts until **YOU** lift it. You can lift for a specified amount of time OR a specified business. After the time has elapsed or the business has viewed the report, the freeze will go back into place. It can also be lifted permanently.

WHO DO I CONTACT? See page 3 for detailed instructions for placing, thawing and lifting the freeze.

FREE CREDIT REPORT MONITORING:




WHAT IS IT? Credit report monitoring is when a third party monitors your credit reports for suspicious activity and identity theft red flags.

HOW LONG WILL IT LAST? & WHO DO I CONTACT? Check the security breach notice you receive for more information on opting in and the duration of the service. *If a monitoring product is not offered and you would like to have one, be sure to do your research and find the best fit for you.*

★**REMEMBER:** All of these tools are independent of one another. That means you **MUST** opt into them separately. The freeze and fraud alert only mitigate the effects of identity theft related to products or services where your credit report is viewed as part of the application process.

How to *Place*, *Thaw* or *Lift* a Security Freeze

You **MUST** contact EACH credit reporting agency to place, thaw or lift the freeze.

	EQUIFAX	EXPERIAN	TRANSUNION
 Place a Freeze	<p>Online: https://www.freeze.equifax.com</p> <p>Phone: 800-685-1111 (automated line- press 3)</p> <p>Mail*: Equifax Security Freeze PO Box 105788 Atlanta, GA 30348</p>	<p>Online: https://www.experian.com/freeze</p> <p>Phone: 888-397-3742 (automated line- press 2; press 2 for Fraud Prevention, press 2 for Security Freeze)</p> <p>Mail*: Experian Security Freeze PO Box 9554 Allen, TX 75013</p>	<p>Online: https://freeze.transunion.com</p> <p>Phone: 800-680-7289 (automated line- press 3)</p> <p>Mail*: TransUnion, LLC PO Box 6790 Fullerton, CA 92834</p>
 Temporarily Lift	<p>You can thaw using same methods as above. Be sure to have your PIN available.</p> <p>THE CREDIT REPORTING AGENCIES MUST THAW THE FREEZE WITHIN 15 MINUTES OF YOUR REQUEST.</p>		
 Permanently Lift	<p>You can permanently lift a freeze using the same methods as placing it. Be sure to have your PIN available.</p>		

Want to thaw a freeze by mail? *
Provide the same information requested when you placed the freeze, plus:

- Your PIN and
- The specific creditor you are thawing the report for or
- The time period you would like it thawed for (ie: date range).

Want to lift a freeze by mail? *
Provide the same information requested when you placed the freeze, plus:

- Your PIN and
- Two types of identification.

* When using the mail-in option, we recommend sending the letter certified mail, return-receipt requested.

Also, the following items need to be submitted with a mailed request:
your name, including any suffix (e.g. Jr. Sr.), complete address, SSN, date of birth, COPY of an item to validate your ID (Valid driver's license, pay stub, W2 or 1099 form.)

Get in the Habit

Everyday practices that help you avoid identity theft.

Like to surf the web, shop or bank online?

- Use anti-virus software and update it often.
- Don't use public wi-fi to make purchases or login to your mobile banking site.
- Be suspicious of e-mails or texts that have bad grammar and encourage you to click on a link or download something.




Stay ON GUARD Online!

Request your **FREE** annual credit report!



It's easy, FREE and you get 3 each year; one from Equifax, Experian and TransUnion.
Just call 877-322-8228 OR visit www.annualcreditreport.com

DO these things:



-  Use strong passwords! Try to include lowercase and upper case letters as well as numbers and symbols.
-  Take those outgoing bills to a USPS blue mailbox.
-  Shred items that include personal information before getting rid of them.

DON'T do these things:

-  Never release your personal identifying information (PII) to someone you don't know. That means keep your SSN, date of birth and financial account numbers to yourself! Look out for callers, text messages and e-mails trying to get PII.
-  Don't carry around your social security card or birth certificate.



SCAM ALERT!



Scammers follow the headlines!

If they know a breach has occurred, it can lead to calls, e-mail or texts that either attempt to get your information or your money. Do not give your personal information to someone who calls or e-mails you.



Watch out for phishing e-mails!

If you signed up with a monitoring service, look out for phishing e-mails with subject or content saying things like: **"Identity Theft Alert"** or **"Your Score Has Dropped."** Verify that the e-mail is from your credit monitoring service before replying or clicking any links.

Are You a Victim of Identity Theft?

In addition to placing a fraud alert and a security freeze on your credit reports:

CLOSE AFFECTED/FRAUDULENT ACCOUNTS AND DISPUTE THEM:

- Get dispute forms from the companies.
- Send the form certified mail, return receipt requested.
- Once the dispute process is complete, ask for a letter that confirms the accounts and fraudulent debts are resolved.
- Keep copies of ALL correspondence for your personal records.
- Are signs of fraud showing up on your credit report? Send a letter explaining the errors/mistakes to the 3 credit reporting agencies, too.

FILE A COMPLAINT WITH THE FTC:

The Federal Trade Commission shares complaint data with law enforcement officials nationwide.

- You need the complaint affidavit to serve as part of your official "ID Theft Report" for disputing any further fraudulent activity. Report to 877-438-4338 or ftc.complaintassistant.gov.

FILE A POLICE REPORT:

Take your FTC affidavit with you. If the officer is hesitant to fill out the report, request an information only report. You need the police report to complete your ID Theft Report.

Remember!

When resolving ID Theft, keep detailed records.



- Create a phone log and note who you talked to and when.



- Send letters by certified mail, return receipt requested.



- When sending supporting documents, send copies, not originals.



- Be aware of deadlines or time constraints.

Common Ways Thieves Use **Your** Identity

Medical Identity Theft. If an identity thief receives treatment in your name, their medical information - like blood type, test results or allergies - can get into your medical file. If you suspect someone has used your medical information:

- Contact each health care provider and ask for copies of your medical records.
- Review your records and report errors to your health care provider.
- Notify your health insurer and all 3 credit reporting agencies.

Misuse of Social Security Number. An identity thief may steal your SSN and sell it, or use the number to get a job or other benefits. Contact the Social Security Administration when you discover any misuse of your social security number.

- 800-269-0271
- www.socialsecurity.gov
- Social Security Administration
Fraud Hotline, PO Box 17785, Baltimore, MD 21235

Income Tax Fraud. If you think that someone has misused your SSN to get a job or tax refund - or the IRS sends you a notice indicating a problem - contact the IRS immediately.

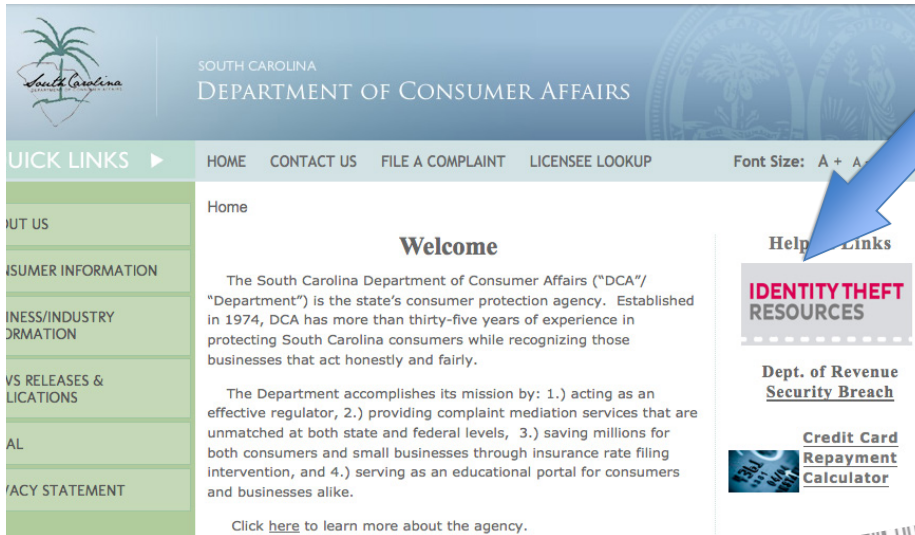
- IRS Identity Protection Specialized Unit: 800-908-4490 or www.irs.gov/identitytheft
- Report the fraud and request the IRS ID Theft Affidavit Form 14039.
- Send a copy of your police report and proof of identity (i.e. copy of driver's license) Fraud Hotline, PO Box 17785, Baltimore, MD 21235

Knowledge is POWER!

Use these resources to your advantage.

FIND THE FOLLOWING PUBLICATIONS ON OUR IDENTITY THEFT RESOURCES PAGE:

www.consumer.sc.gov



Publications:

Consumer Alert: Special Edition-ID Theft
ID Theft: What to Do if it Happens to You
How to Place, Thaw or Lift a Security Freeze
Notifying the Credit Bureaus of a Death
Minimize the Effects of ID Theft
"Credit Alert" Phishing E-mails

Videos:

ID Theft: Why it Should Matter to You!
Worried about Identity Theft?



FOR MORE INFORMATION ON ID THEFT AND VARIOUS OTHER TOPICS, VISIT:



Check out our
YouTube channel.
youtube.com/scdcatv



Look here for updates &
educational materials.
facebook.com/scdca



Find the latest scam
alerts and news here.
twitter.com/scdca

SCDCA aims to protect consumers from inequities in the marketplace through advocacy, complaint mediation, enforcement and education.



South Carolina Department of Consumer Affairs
2221 Devine St. • STE. 200 • PO Box 5757 • Columbia, SC 29250
1-800-922-1594 • www.consumer.sc.gov



Checklist & Notes

☐ **Fraud Alert**
Date Placed: _____

Credit reports requested after placing Fraud Alert:

☐ Experian - Date Requested_____ Date Received_____

☐ TransUnion - Date Requested_____ Date Received_____

☐ Equifax - Date Requested_____ Date Received_____

☐

Security Freeze

☐ Experian - Date Placed_____PIN_____

☐ TransUnion - Date Placed_____PIN_____

☐ Equifax - Date Placed_____PIN_____

NOTES

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



Summer 2013